ORIGINAL

BEFORE THE

Federal Communications Commission

WASHINGTON, D.C.

In the Matter of Policies and Rules Concerning Toll Fraud	))))	CC Docket No. 93-292

TO: The Commission

COMMENTS

Quantum Logic, Inc. ("Quantum Logic"), by its attorneys and pursuant to Section 1.429 of the Commission's Rules, hereby submits its Comments on the Notice of Proposed Rulemaking ("NPRM") released December 2, 1993, in the above-captioned docket.

Quantum Logic is interested in the problem of toll and roamer fraud and seeks to introduce new technology to detect and prevent such fraud. It shares the Commission's goals "to find solutions to each fraud problem without hindering the development or use of" new technologies and "ensur[ing] that telecommunications equipment and services remain accessible."[1/] To that end, Quantum Logic is developing a detection system which will allow the telecommunications industry to control access to its networks and to prevent fraud.

The detection system, known as the Fingerprint Identification System[2/] ("FIDS"), will enable telecommunications

---

1/ NPRM at para. 5.

2/ International patents pending.

providers to ascertain almost immediately whether the attempted user is authorized to use its system. The user will scan his fingertip over a small electronic device that will convert the fingerprint image into an eight byte encrypted binary access key. The network's computers will then compare the transmitted user's access key to the authorization keyfile before access is allowed.

Attached is a report from Quantum Logic which further details the benefits of this new technology. Quantum Logic applauds the Commission's efforts, as evidenced by this rulemaking proceeding, to stem the growing problem of toll and roamer fraud.

Respectfully submitted,

QUANTUM LOGIC, INC.

By: _____
Eliot J. Greenwald
Julie Arthur Garcia

Its Attorneys

FISHER, WAYLAND, COOPER
and LEADER
1255 23rd Street, N.W.
Suite 800
Washington, DC 20037
(202) 659-3494

Dated: January 14, 1994

FINGERPRINT IDENTIFICATION SYSTEM*

A Unique Method of Avoiding
Telecommunications Fraud

E. Michael Clough
Robert Beers
Daniel Richards
QUANTUM LOGIC, INC.
7901 Flying Cloud Drive
Suite 250
Minneapolis, MN 55344
(612) 942-7650

* International Patents Pending

FINGERPRINT IDENTIFICATION SYSTEM*/

Toll and roamer fraud is costing the telecommunications industry billions of dollars annually. Thanks to new technology from Quantum Logic, Inc., this type of fraud can be minimized through industry control over access to its systems. Controlling access to a communications network and thereby preventing fraud requires quick identification of whether and to what extent a user is authorized to use the network. Without the ability to identify authorized users, the fraud problem will escalate.

Toll and roamer fraud occurs in many ways. It can occur through customer-controlled devices such as a PBX. It can occur through cellular cloning, a process by which the perpetrator of fraud picks up the Electronic Serial Number ("ESN") and Mobile Identification Number ("MIN") of an authorized user as it is transmitted over the airwaves. Toll fraud can occur when long distance calling cards are lost or stolen, or when a personal identification number ("PIN") is simply copied off the card. There are currently no effective methods available to protect against these, and other types, of toll and roamer fraud.

The assignment of financial responsibility for such fraud is an increasingly complex issue. Quantum Logic, Inc. believes, however, that assigning responsibility is not the important issue. In the long run, it is the consumer who will pay for losses due to fraudulent activities through increased service costs. Therefore, the telecommunications industry should focus

---

*/ International Patents Pending

on the prevention of fraud rather than passing on the loss to its customers as an operational cost.

Not surprisingly, there is only one reliable method of preventing fraud: total access control. The telecommunications industry requires a method by which to tie the actual user to the activity on the network, and thereby assign cost in the appropriate fashion. The challenge confronting the industry at this time is to determine a practical method of positively identifying the individual user by some unique characteristic that cannot be stolen, cloned, electronically simulated or otherwise duplicated.

Voice recognition, once thought to be a solution to fraud problems, does not offer a viable long-term solution, particularly in digital access. Voices are altered through technology as simple and widely used as telephone or radio circuits. Voice recognition in high security situations requires expensive and time-consuming on site analysis of the unique characteristics of an individual's voice prior to transmission. An easier and more efficient solution is urgently needed; Quantum Logic, Inc.'s new fingerprint matching technology solves this need.

Fingerprint matching is the most widely accepted system of identification, other than DNA analysis, used by law enforcement officials. No two individuals have identical fingerprints, and it is a unique physical characteristic that is difficult to alter. Therefore, a method of fingerprint identification offers the measure of security necessary to prevent fraud.

Fingerprint recognition as protection against telecommunications fraud has many benefits. Fingerprint patterns can be quickly scanned and converted to a video image, which can then be compared with a data base of authorized prints. A system of identification of minutiae points accelerates the classification of the unique characteristics of a fingerprint and thereby accelerates the process of matching prints. A method of scanning the finger and converting the minutiae points into a computer-compatible format was developed in which a raster image of the fingerprint is converted into a binary format. This enables computers to match prints through a comparative process. Calling cards, personal identification numbers and the like, which can be easily lost, stolen or copied, become unnecessary. The would-be perpetrator of fraud can be clearly identified and his fingerprints possibly matched with the data bases of law enforcement offices for prosecution.

Fingerprint technology has evolved from early, time-consuming and less accurate methods of fingerprint matching that required human intervention to today's fast, efficient automated process. By utilizing a new technology known as the Fingerprint Identification System ("FIDS") (international patents pending), Quantum Logic, Inc. has eliminated the problems inherent in applying fingerprint recognition to access control. Previously, problems such as pressure distortion and orientation of a finger when placed on an optical scanner, and surface contaminations on a fingerprint, seen as scratches or cuts, decreased the

reliability of the fingerprint match, resulting in false acceptance and false rejections.

The FIDS method solves these problems by scanning the finger with a small video camera to develop an image that can be converted into vector information. The process of vector analysis results in coordinate information about vector line types. The mapping of coordinate data representing the vector line types, or minutiae points, is converted into an eight byte encrypted binary access key and sent to the network's control system within two seconds. This results in an accurate, cost-effective, high performance identification system. Computers can more quickly match access keys that result from vector information because the FIDS method eliminates the need for large data files inherent in other processes, thereby increasing overall speed.

The ability to control access to a telecommunications system provides the obvious anti-fraud benefits, and also opens up the potential of offering vertical services to users. Users can subscribe to specific levels of service access within the same network and the provider can determine through fingerprint technology the user and the level of service to which access should be granted. The FIDS method offers a secure, cost-effective, high performance access control system that can be implemented in the telecommunications industry.